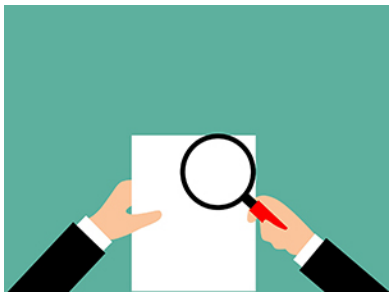
What Documentation Should You Review for a Critical Vendor?

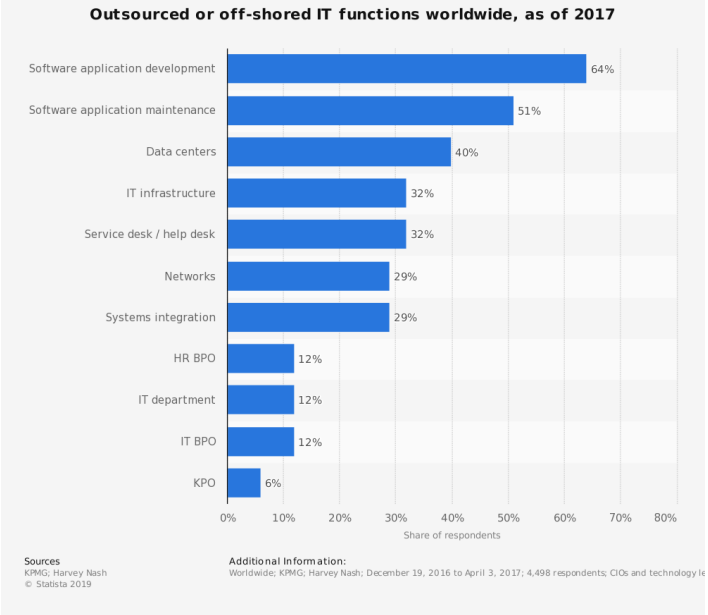
Written by: Jon Waldman
Partner, EVP of IS Consulting - SBS CyberSecurity, LLC



15 years ago, many of the products and services used by organizations were still being purchased at a retail shop. Remember those boxes that contained a CD (or a few CDs – before that: floppy drives!) that you had to go around and painstakingly install on EACH workstation? Let's not even talk about having to update or upgrade that software… yuck.

Today, nearly everything lives in "the cloud." Having someone else store, manage, monitor, update, patch, and maintain your applications, data, networking devices, servers, and sometimes your entire infrastructure can add risk to your organization, but it can also save you time, money, and resources. Additionally, outsourcing a business process can, in many cases, mitigate risk to your business by adding specialized expertise that you don't already possess, such as better (and often more secure) IT infrastructure management and support, network monitoring, custom software development, data analytics, or social media marketing.

Outsourcing can also give you a competitive advantage in your market and get your business access to products and services you wouldn't be able to adopt as quickly on your own. According [to Deloitte's 2018 Global Outsourcing Survey](), approximately 84 percent of the 500 survey respondents have either initiated discussions, conducted pilots, or have implemented at least some disruptive solutions.



Outsourced IT Functions, as of 2017

The Goal of Vendor Management

The reason we do any risk assessments in the first place is to help you to make a better decision. In the world of lending, the Loan Risk Assessment helps you to understand how risky the loan is going to be to your organization and what you can do to mitigate that risk. The same holds true with a Vendor Risk Assessment. Your Vendor Risk Assessment should tell you your most important/critical vendors, your most risky vendors (not always the same as your most important vendors), and whether or not you want to continue doing business with that vendor based on the risk they pose to your organization.

But how do you get assurance that a particular vendor is properly protecting your confidential customer information?

Short of physically auditing or inspecting a vendor yourself, the best way to gain confidence in your vendor's security posture is through the gathering of security-related documentation. Your most important and critical vendors are typically going to be subject to regulatory guidance themselves, which includes having their own independent testing performed as well as undergoing their own IT Exams. Core banking providers, for example, are examined by federal regulatory agencies similarly to most financial institutions (see the FFIEC Supervision of Technology Service Providers booklet for more information).

So then – what types of documentation should you be looking for from a vendor to provide you reasonable assurance that the vendor is protecting your data? Let's dive into the two major components of vendor documentation to review: Due Diligence documentation and contracts.

Due Diligence Documentation to Gather (According to Regulation)

The goal of Due Diligence documentation review is to dig into what a vendor is doing to both protect your data and to stay a viable business. Here's a listing of vendor Due Diligence documents to gather (and what to look for) based on regulatory guidance (FFIEC, FDIC, OCC, Federal Reserve):

- **An assessment of Information Security or Information Technology controls**
  - The most common report in this category is an SSAE-18 or SOC Report. To get any good security information, however, you should insist on a SOC 2 Type II report, which is based on the Trust Services Criteria, rather than controls around financial reporting (SOC 1 reports)
  - Keep in mind that a SOC report is not required by any law or regulation, but is an expectation of most large service organizations (your vendors)

- Alternatively, if a vendor does not have a SOC report, an independent, external IT Audit of some sort is your next best bet
- For more information about extracting valuable security information from SOC 2 reports, check out SBS' 2-part Hacker Hour here:
    - Part 1: https://sbscyber.com/resources/hacker-hour-develop-a-better-understanding-of-soc-2-reporting
    - Part 2: https://sbscyber.com/resources/special-request-hacker-hour-understanding-soc2-reviews-part-2

Risk Management

- Review your vendor's SOC 2 report for information about their risk management program, including areas of risk management and responses to risky areas
- If the vendor does not have a SOC 2 report, ask to see their most recent risk assessment(s)
- From OCC 2013-29: Evaluate the effectiveness of the third party's risk management program, including policies, processes, and internal controls

- **Information Security Program**
    - Review your vendor's SOC 2 report for information about their Information Security Program, including the areas of information security governance to which the vendor holds themselves
    - If the vendor does not have a SOC 2 report, ask to see their most recent Information Security Program
    - From OCC 2013-29: Assess the third party's information security program. Determine whether the third party has sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities. When technology is necessary to support service delivery, assess the third party's infrastructure and application security programs, including the software development life cycle and results of vulnerability and penetration tests

- **Business Continuity Plan**
    - Review your vendor's SOC 2 report for information about their Business Continuity Plan, including documentation around how the vendor plans to continue their business operations AND support your institution in the event of a disaster or outage
    - If the vendor does not have a SOC 2 report, ask to see their most recent Business Continuity Plan
    - From FFIEC OTS: Ability to meet disaster recovery and business continuity requirements (FFIEC OTS)
    - From FDIC FIL 44-2008: Business resumption strategy and contingency plans
    - From OCC 2013-29: Assess the third party's ability to respond to service disruptions or degradations resulting from natural disasters, human error, or intentional physical or cyber attacks. Determine whether the third party maintains disaster recovery and business continuity plans that specify the time frame to resume activities and recover data

- **Incident Response Plan**
  - Review your vendor's SOC 2 report for information about their Incident Response Plan, including documentation around how the vendor plans to prevent, detect, or recover from internet or cyber-based incidents
  - If the vendor does not have a SOC 2 report, ask to see their most recent Incident Response Plan
  - From OCC 2013-29: Review the third party's incident reporting and management programs to ensure there are clearly documented processes and accountability for identifying, reporting, investigating, and escalating incidents

- **Insurance Coverage**
  - Make sure your vendor's insurance coverage is adequate to cover any losses that you may incur due to a failure on the vendor's part
  - From OCC 2013-29: Verify that the third party has fidelity bond coverage to insure against losses attributable to dishonest acts, liability coverage for losses attributable to negligent acts, and hazard insurance covering fire, loss of data, and protection of documents

- **Audited Financials**
  - Make sure your vendor's financial documentation shows that they are a healthy, growing company that will be around to support your organization for a long time
  - From FFIEC OTS: Financial status, including reviews of audited financial statements
  - From FDIC FIL 44-2008: Audited financial statements, annual reports, SEC filings, and other available financial indicators
  - From OCC 2013-29: Assess the third party's financial condition, including reviews of the third party's audited financial statements. Evaluate growth, earnings, pending litigation, unfunded liabilities, and other factors that may affect the third party's overall financial stability

What to Look for in a Contract (According to Regulation)

One of the greatest areas of concern during the outsourcing process is the contract. No surprise to anyone here, but most contracts are written BY the vendor FOR the vendor. Customers (you) need to review those contracts before signing them to ensure YOUR interests are also being protected. Here's a listing of areas to look for in a contract, based on regulatory guidance (FFIEC, FDIC, OCC, Federal Reserve):

- **Nature and Scope of Arrangement:** The contract should clearly set forth rights and responsibilities of the contract, including timeframes, frequency, support, training, maintenance, etc.

- **Performance Measures or Benchmarks:** Otherwise known as Service Level Agreements – does the vendor document a level of service to which you can hold that vendor? What's the expected uptime or hours of training or support provided?
- **Responsibilities for Providing, Receiving, and Retaining Information:** What types of reports and information will the vendor provide to you? Examples include performance reports, control audits, financial statements, security reports, BSA/AML and Office of Foreign Asset Control (OFAC) compliance responsibilities and reports for monitoring potential suspicious activity, reports for monitoring customer complaint activity, and business resumption testing reports.
- **The Right to Audit and Require Remediation:** Make sure the contract establishes your right to audit, monitor performance, and require remediation when issues are identified.
- **Responsibility for Compliance with Applicable Laws and Regulations:** Pretty straight-forward; make sure the vendor is subject to the same laws and regulations to which you are held.
- **Cost and Compensation:** Make sure all fees are described and accounted for, including any conditions under which the cost structure may be changed.
- **Ownership and License:** Make sure the contract states that YOU are the owner of YOUR data, not the vendor.
- **Confidentiality and Integrity:** Prohibit the vendor (and its subcontractors) from using or disclosing YOUR data, except as necessary to comply with legal or law enforcement requirements.
- **Business Resumption and Contingency Plans:** Ensure the vendor is contractually bound to maintain a Business Continuity/Contingency Plan, as listed in the Due Diligence section.
- **Indemnification:** Make sure that you understand where and when the vendor can be held liable in the event of a failure of the vendor to perform and ensure your institution is not liable for any failure of the vendor to perform.
- **Insurance:** The vendor should be contractually obligated to hold adequate insurance, notify you of material changes to coverage, and provide evidence of coverage where appropriate.
- **Dispute Resolution:** How will disputes be resolved expeditiously (arbitration, mediation, or other means) and will the vendor continue to provide services during any disputes?
- **Limits on Liability:** Does the contract limit the liability of the vendor, and is any liability limit proportional to the loss you might experience due to a vendor failure?
- **Default and Termination:** BIG focus here in the last few years. What constitutes default, and what recourse does your institution have if a vendor is no longer able to provide services as expected? Can you terminate the relationship (for cause) without prohibitive expenses? How do you get your data back? What does the vendor do with your data once the relationship has been terminated?
- **Customer Complaints:** Who is responsible for handling customer complaints that arise from the services provided by the vendor? If the vendor is handling such complaints, how are they reported to you?
- **Subcontracting/Multiple Service Provider Relationships**: When (and how) should the vendor notify you when using subcontractors, as it relates to the products and services you receive from the vendor?

- **Foreign-Based Third Parties:** If the vendor is foreign-based, is the vendor contractually obligated to follow US laws and regulations? If not, seek legal advice to determine the ramifications of such an arrangement.
- **Regulatory Supervision:** Is the vendor contractually obligated to be examined by a US federal regulatory agency?

That's a lot of stuff to consider in contracts, but once again, make sure you're protecting your organization, because the vendor isn't going to be looking out for you in a contract.

Furthermore, the FDIC recently released FIL -19-2019 – Technology Service Provider Contracts - reminding institutions that long-term and automatically renewing contracts may put your institution at a higher risk, as those older contracts likely won't have much of these modern contractual considerations. Don't just let old contracts be old contracts. Talk to your vendors and work on mitigating your risk.

Be sure to check out SBS' breakdown of FDIC FIL-19-2019 here:
https://sbscyber.com/resources/technology-service-provider-contracts-fil-19-2019

Some Alternative Documentation to Gather (Modern, Non-Regulation Stuff)

Most of the regulatory guidance available today was written in 2013 or before (the FFIEC OTS booklet is from 2004; we need an update, guys!). While the regulatory guidance is helpful, here are a few additional Due Diligence documents you should consider adding to your MODERN Vendor Management required-documents list:

- **Results of Penetration Tests:** Is the vendor regularly testing their external perimeter network from internet-based cyber attacks, testing for attacks that today's hackers would use?
- **Results of Vulnerability Assessments:** Is the vendor regularly scanning their network devices for known vulnerabilities to ensure they are both protected and doing a good job of patch management?
- **Results of Social Engineering Assessments:** Is the vendor regularly testing their people to determine if security awareness testing is having a positive effect against known Social Engineering attacks like phishing emails or phone impersonation?
- **Web Application Assessment Reports:** Has the vendor reviewed the code of their internet-facing web applications to defend against modern web attacks, like cross-site scripting, SQL injection, or remote code execution?
- **Results of Online Vendor Security Assessments**: There are many modern online vendor security assessments that can provide you insight into a vendor's online presence and overall security posture, such as Security Scorecard, UpGuard, SSL Labs, or Mozilla's Observatory.
- **Results of Business Continuity or Incident Response Testing:** Has the vendor tested their Business Continuity or Incident Plans through either tabletop walkthroughs or functional testing? Has the vendor made improvements to these plans based on those results?

What Happens When Documentation Isn't Good?

The goal of a Vendor Risk Assessment or review is to determine whether or not you want to continue doing business with that vendor. If the answer is "yes, this vendor is within our acceptable levels of risk," then great! That vendor gets a gold star and two thumbs-up; then you move on to the next review.

If a vendor provides you documentation that contains numerous red-flags or issues – or worse yet, doesn't provide you requested documentation – then that vendor's risk must be increased. If there are enough issues, red flags, or missing requested documents, then SBS recommends placing that vendor on a Watch List.

Your organization might have a Watch List for other areas where a thing (loan, credit card, customer, etc.) has an elevated risk level, and this vendor Watch List serves the same purpose.

You must choose how you want to handle this elevated risk. You can do one of three things:

1. **Accept the Risk:** Stay with the vendor as-is, but document this now-known risk(s) and report upstream. It's ok to accept risk, as long as you make sure the rest of the organization is aware of this increased risk and monitor the risk closely going forward.
2. **Mitigate the Risk:** Work with the vendor to address the known risk(s) or receive the documentation they didn't get you in the first place. Once the risk is mitigated (fixed) or the documentation received, the vendor can come off the Watch List.
3. **Change the Risk:** Simply put, find a new vendor, or stop using the product/service that the vendor provides.

A Culture of (Vendor) Security

Just as building a culture of good security at your organization is an extremely important component to protecting customer information holistically, a vendor's culture of security – i.e., their willingness to discuss security, share security information, and provide results of security testing – is going to be a major factor in the world of vendor management going forward.

As information and cybersecurity continue to take a more prominent role in society and business, vendors, too, are having to become more security conscious. In our experience, a vendor that is not willing to share security information up-front or be transparent about security findings and plans to resolve recommendations should raise some big red flags immediately. If it's like pulling teeth to get any good security information from a particular vendor, the odds are it'll be like pulling teeth to get good customer service, changes or fixes to products/services, or needed training and education as well.

If you ask a vendor about security information, and they say, “we’re glad you asked! Let’s talk about what we do to help secure your data,” the odds that you’re going to be better protected, have a responsive vendor, and get better customer service are much better.

Cybersecurity is a tremendously important topic in today’s world of data breaches and ransomed networks. Existing vendors can either step up their security game, or the market will shift to new vendors that are more transparent.

SBS Resources

- **{Service} Full Service Vendor Management:** SBS security experts will get to work for you by taking on the daunting responsibility of vendor management. Your organization will be able to make better data-driven security decisions without having to do all the background work.
- **{Solution} TRAC:** Make better decisions and easily perform four major components of vendor management: risk assessment, selection, review, and contract management with the TRAC Third Party Management module.
- **{Certification} Certified Banking Vendor Manager:** The online Certified Banking Vendor Manager (CBVM) course includes real-world exercises to build a comprehensive, time-saving vendor management program to take back to your institution. With this certification you will become a trusted vendor management expert in the eyes of your organization, as well as your auditor or examiner.

Contact Rick Olivier to learn more about how SBS can help with any of your vendor management needs.

- Rick.olivier@sbscyber.com
- (605) 270-3321